



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/482,840	01/13/2000	Marcus Peinado	MSFT-0109/127334.9	7581

7590 05/18/2004  
Steven H Meyer  
WOODCOCK WASHBURN KURTZ MACKIEWICZ & NORRIS LLP  
One Liberty Place  
46th Floor  
Philadelphia, PA 19103

EXAMINER

NGUYEN, CUONG H

ART UNIT PAPER NUMBER

3625

DATE MAILED: 05/18/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/482,840

Applicant(s)

PEINADO ET AL.

Examiner

CUONG H. NGUYEN

Art Unit

3625

MW

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 21 April 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 106-181 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 106-181 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)             | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)    | Paper No(s)/Mail Date. _____  |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____   | 6) <input type="checkbox"/> Other: _____                                    |

**DETAILED ACTION**

1. This Office Action is the answer to the communication received on 8/19/2002 (the Supp. IDS).
2. Claims 106-181 are pending in this application

**Drawings**

3. This application has been filed with formal drawings which currently are acceptable for examining purposes.

**Response**

4. The previous rationales and references for 35 USC 103(a) rejections are withdrawn due to a new ground of rejection (Downs et al., US Pat. 6,226,618). The examiner regrets for a delay in the examining process.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. § 103(a) which forms the basis for all obviousness rejections set forth in this Office Action:

*(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.*

5. First of all, it is known with one of ordinary skill in the art that a DRM system obviously contains a structure/"box" with encryption/decryption keys inside (as claiming a digital right management having encryption/decryption keys (or a public/private key pair which is similar to encryption/decryption keys)).

Downs et al. (US Pat. 6,226,618) disclose in **the description of the related art** portion: "Further information on the background of protecting digital content can be found from the

following three sources. "Music on the Internet and the Intellectual Property Protection Problem" by Jack Lacy, James Snyder, David Maher, of AT&T Labs, Florham Park, N.J. available online URL

<http://www.a2bmusic.com/about/papers/musicipp.htm>. **Cryptographically**

**protected container**, called **DigiBox**, in the article "Securing the Content, Not the Wire for Information Commerce" by Olin Sibert, David Bernstein and David Van Wie, InterTrust Technologies Corp. Sunnyvale, Calif. available online URL

<http://www.intertrust.com/architecture/stc.html>. And "Cryptolope Container Technology", an IBM White Paper, available online URL <http://cyptolope.ibm.com/white.htm>.

- A DRM system (109) of Downs et al. has all features of claim 106, Downs et al. disclose "5. End-User Device(s) 109 The End-User Device(s) 109 can be any player device that contains an End-User Player Application 195 (described later) compliant with the Secure Digital Content Electronic Distribution System 100 specifications. These devices may include PCS, set top boxes (IRDs), and Internet appliances. The End-User Player Application 195 could be implemented in software and/or consumer electronics hardware. In addition to performing play, record, and library management functions, the End-User Player Application 195 performs SC processing to enable rights management in the End-User Device(s) 109. The End-User Device(s) 109 manages the download and storage of the SCs containing the Digital Content; requests and manages receipt of the encrypted Digital Content keys from the Clearinghouse(s) 105; processes the watermark(s) every time the Digital Content is copied or played; manages the number of copies made (or deletion of the copy) in accordance with the Digital Content's Usage Conditions; and performs the copy to an external media or portable consumer device if permitted. The portable consumer device

can perform a subset of the End-User Player Application 195 functions in order to process the content's Usage Conditions embedded in the watermark. The terms End-User(s) and End-User Player Application 195 are used throughout this to mean through the use or running-on an End-User Device(s) 109".

A. Claims 106-111: They are rejected under 35 U.S.C. § 103(a) as being unpatentable over Downs et al. (US Pat. 6,226,618).

Downs et al. teach a method of obtaining a structure having encryption/decryption keys, comprising:

- requesting encryption/decryption keys (see **Downs**, in 7:55-58, "Only users who have decryption keys can unlock the encrypted Content, and the Clearinghouse(s) releases decryption keys only for authorized and appropriate usage requests."

- generating, a public/private key pair (or in other words, encryption/decryption keys), (see **Downs** 15:50-52, "Process Flow for Encryption Process of FIG. 3

Step	Process
301	Sender generates a random symmetric key and uses it to encrypt the content

";

- delivering encryption/decryption keys (see **Downs**, Fig. 1D, this teaches a step of delivering and installing (E) the black box (194) in a DRM system); and installing encryption/decryption keys in a DRM system.

- Downs et al. teach that in 15:2-15, "Detailed Description Text (69): This document uses a drawing to graphically represent SC(s) that shows encrypted parts, non-encrypted parts, the encryption keys, and certificates. Referring now to FIG. 2 is an example drawing of SC(s) 200. The following symbols are used in the SC(s) figures. Key 201 is a public

or private key. The teeth of the key e.g. CLRNGH for Clearinghouse indicate the key owner. PB inside the handle indicates that it is a public key thus key 201 is a Clearinghouse public key. PV inside the handle indicates that it is a private key. Diamond shape is an End-User Digital Signature 202. The initials indicate which private key was used to create the signature thus in EU is the End-User(s) digital signature from table below. Symmetric key 203 is used to encrypt content.”.

It is reasonable that different modifications of the described suggestions of Downs et al. would be apparent to those skilled in the art without departing from the scope and spirit of their disclosures (this pending case has a Sensitive Application Warning system issues from USPTO because it pits MicroSoft against IBM). It should be understood that their suggestions should not be limited to specific embodiments in said disclosures.

It would have been obvious to one of ordinary skill in the art at the time of invention to implement the system of Downs et al. to claim a method using a DRM system to obtain a black box from a server (143-144) including requesting (D) a black box, creating a black box and delivering and installing (E) the black box (194) in the DRM system (109) because these particular available information would improve a level of security for a digital right management system.

B. Claim 107: This claims about the method of claim 106

wherein the DRM system has a previously installed structure relating to (encryption/decryption keys) prior to the requesting step, the method further comprising determining

prior to the requesting step that the previously installed structure is non-unique.

The rationales and reference for rejection of claim 106 are incorporated.

The examiner submits that it is obvious to one with skill in the art to utilize Downs et al. ideas to edit if there is a critical difference in previously procedure (i.e., edit if previously installed black box is not current") procedure because the order is still logic/reasonable/making sense. It would be obvious to artisans that a step of "determining prior to the requesting step that the previously installed structure is non-unique" have been known to be easily done to avoid any possible error/conflict in computer world (furthermore, the claimed phrase is merely about an intent of use with a box containing public/private key pair and not contributing to a step of obtaining a black box, this is obvious to one with ordinary skill in the art as an application for a particular purpose).

C. Claim 108: This claims about the method of claim 106 wherein the DRM system has a previously installed structure prior to the requesting step, the method further comprising determining prior to the requesting step that the previously installed structure is not current.

The rationales and reference for rejection of claim 106 are incorporated.

The examiner submits that this claimed step is obviously analogous to claim 107's limitation because a step of "checking if encryption/decryption key is unique" is similar to "checking to see if said keys are current or not"; therefore, similar rationales and reference for an obviousness rejection of claim 107 are applied.

D. Claim 109: The rationales and reference for rejection of claim 106 are incorporated.

This claims about the method of claim 106 with requesting the structure (a unique public/private key pair (for performing the decryption and encryption functions)) by way of a network connection to a server (see **Downs** et al., 1:62-67).

E. Claim 110: The rationales and reference for rejection of claim 109 are incorporated.

This claims about the method of claim 109 wherein the requesting step comprises requesting the structure by way of an Internet connection to the structure server (see **Downs** et al., 1:62-67).

F. Claim 111: This claim's limitations are obviously analogous to limitations of claim 106 (**merely claiming providing a box having public/private key pair**). Therefore, similar rationales and references set forth are applied for a rejection under 35 U.S.C. § 103(a).



G. Claim 112: The rationales and reference for rejection of claim 111 are incorporated.

This claims about the method of claim 111 wherein the DRM system had a second previously installed structure prior to having the first previously installed structure, the second previously installed structure having a public/private key pair different from the public/private key pair of the first previously installed structure and also different from the public/private key pair of the generated structure, and wherein the generating step further includes providing the generated structure with the public/private key pair of the second previously installed structure.

The examiner submits that this claimed step is obviously analogous to claim 111's limitation because analogous repetition of a step is claimed (i.e., merely providing a box with a public/private key pair); therefore, similar rationale and reference are applied.

H. Claim 113: The rationales and reference for rejection of claim 106 are incorporated.

This claims about the method of claim 106 wherein the generating step is capable of identifying a current status.

Downs et al. teach about checking a current status in Detailed Description Text (para. 323):

" Any problem discovered, even minor text changes requires that the SC(s) be rebuilt due

to internal security features of SC(s). To avoid unnecessary re-processing time, it is highly recommended that the interim quality assurance steps be utilized to assure accuracy of the metadata and that this specific quality assurance step be reserved for validating appropriate cross references between the SC(s) associated with this song. If problems are found, the assurer can enter a problem description to be attached to the song and have it re-queued to the appropriate processing queue for reprocessing. Status is updated appropriately in the Work Flow Manager 154 to indicate the status of all related components of the song. If no problems are discovered, the Content 113 is marked or flagged as ready for release” .

and in Detailed Description Text (para. 344) :

“The Content Hosting Router(not shown) resides in the Content Hosting Site(s) 111 and receives all requests from End-User(s) wanting to download Content 113. It performs validation checks on the End-User(s) request to ensure they indeed bought the Content 113. A database is maintained on the status of the Secondary Content Sites that includes what Content 113 is on them and there current status. This current status includes the amount of activity on the sites and whether a site is down for maintenance.”

I. Claim 114: The rationales and reference for rejection of claim 113 are incorporated.

This claims about the method of claim 113 wherein the generating step includes providing the generated structure with a version number. The examiner submits that “a version number” is merely for identification purpose, this limitation does not contribute to a limitation about a

method for obtaining a black box with public/private key pair.

It would have been obvious to one of ordinary skill in the art at the time of invention to implement the system of Downs et al. to claim a method having a version number of a box that contains a public/private key pair because that is a way to index/organize software related materials.

J. Claims 115-116: The rationales and reference for rejection of claim 106 are incorporated.

This claims about the method of claim 106 wherein the generating step includes providing a digital certificate (see Downs et al., "Detailed Description Text (100):

License control requires that the Content Provider(s) 101, the Electronic Digital Content Store(s) 103, and the Clearinghouse(s) 105 have bona-fide cryptographic digital certificates from reputable Certificate Authorities that are used to authenticate those components. The End-User Device(s) 109 are not required to have digital certificates.").

K. Claim 116: The rationales and reference for rejection of claim 115 are incorporated.

The examiner submits that this claim's limitation is similar to claim 115's limitation; therefore, similar rationale & reference for an obvious rejection are applied.

L. Claims 117-118: The rationales and reference for rejection of claim 117 are incorporated.

- Downs et al. teach about encrypting a private key (see "Detailed Description Text (181):

.One Symmetric Key 623 is used for decrypting the watermarking instructions and the other for decrypting the Content 113 and any encrypted metadata. The watermarking instructions are included within the Metadata SC(s) 620 portion in the Order SC(s) 650. The Content 113 and encrypted metadata are in the Content SC(s) 630 at a Content Hosting Site(s) 111. The URL and part names of the encrypted Content 113 and metadata parts, within the Content SC(s) 630, are included in the Key Description part of the Metadata SC(s) 620 portion of the Order SC(s) 650. The Clearinghouse(s) 105 uses its private key to decrypt the Symmetric Keys 623 and then encrypts each of them using the Public Key 661 of the End-User Device(s) 109. The Public Key 661 of the End-User Device(s) 109 is retrieved from the Order SC(s) 650. The new encrypted Symmetric Keys 623 is included in the Key Description part of the License SC(s) 660 that the Clearinghouse(s) 105 returns to the End-User Device(s) 109." - please note that another term for symmetric-key encryption is private-key encryption.

M. Re. to claim 117: The examiner submits that this claim's limitation is similar to claim 118's limitation; therefore, similar rationale & reference for an obvious rejection are applied.

N. Claims 119-121: The rationales and reference for rejection of claim 106 are incorporated.

This claims a feature of a box having a public/private key pair is inoperable on another DRM system. This is obvious with Downs et al.'s system because "a match" for a public/private key pair with its associating DRM system MUST be required (e.g., Downs et al. disclose that "The Clearinghouse(s) 105 verifies that the name of the Content Provider(s) 101 encrypted together with the Symmetric Keys 623 matches the name of the Content Provider(s) 101 in the SC(s) certificate." ) .

O. Claim 120: The examiner submits that this claim's limitation is obvious from claim 119's limitation (i.e., a public/private key pair is generated based on provided information, that key pair is corresponding to a DRM system); therefore, similar rationale & reference for an obvious rejection are applied. The examiner submits that encryption/decryption keys have been known by artisans to be associated with distinct devices for identification purposes.

P. Claim 121:

This claim is about a method of claim 119 wherein the DRM system is a first DRM system, wherein the generating step includes associating 1st structure with a 1<sup>st</sup> device, and associating a 2<sup>nd</sup> structure with a 2<sup>nd</sup> devices. This is obvious by an exact repetition step that claiming in claim 119.

6. Re. to Claims 122, 138, 152, 168: These claims' limitations are obviously analogous to limitations of claim 106 (although a method or a computer-readable medium teaching a similar method is presented). Therefore, similar rationales and references set forth are applied for a rejection under 35 U.S.C. § 103(a).

7. Re. to Claims 125, 139, 155, 169: These claims' limitations are obviously analogous to limitations of claim 109 (although a method or a computer-readable medium

teaching a similar method is presented). Therefore, similar rationales and references set forth are applied for a rejection under 35 U.S.C. § 103(a).

8. Re. to Claims 126, 140, 156, 170: These claims' limitations are obviously analogous to limitation(s) of claim 110 (although a method or a computer-readable medium teaching a similar method is presented). Therefore, similar rationales and references set forth are applied for a rejection under 35 U.S.C. § 103(a).

9. Re. to Claims 127, 141, 157, 171: These claims' limitation(s) are obviously analogous to limitation(s) of claim 111 (although a method or a computer-readable medium teaching a similar method is presented). Therefore, similar rationales and references set forth are applied for a rejection under 35 U.S.C. § 103(a).

10. Re. to Claims 128, 142, 158, 172: These claims' limitations are obviously analogous to limitation(s) of claim 112 (although a method or a computer-readable medium teaching a similar method is presented). Therefore, similar rationales and references set forth are applied for a rejection under 35 U.S.C. § 103(a).

11. Re. to Claims 129, 143, 159, 173: These claims' limitations are obviously analogous to limitations of claim 113 (although a method or a computer-readable medium teaching a similar method is presented). Therefore, similar rationales and references set forth are applied for a rejection under 35 U.S.C. § 103(a).

12. Re. to Claims 130, 144, 160, 174: These claims' limitations are obviously analogous to limitations of claim 114 (although a method or a computer-readable medium teaching a similar method is presented). Therefore, similar rationales and references set forth are applied for a rejection under 35 U.S.C. § 103(a).

13. Re. to Claims 131, 145, 161, 175: These claims' limitations are obviously analogous to limitations of claim 115 (although a method or a computer-readable medium teaching a similar method is presented). Therefore, similar rationales and references set forth are applied for a rejection under 35 U.S.C. § 103(a).

14. Re. to Claims 132, 146, 162, 176: These claims' limitations are obviously analogous to limitations of claim 116 (although a method or a computer-readable medium teaching a similar method is presented). Therefore, similar rationales and references set forth are applied for a rejection under 35 U.S.C. § 103(a).

15. Re. to Claims 133, 147, 163, 177: These claims' limitations are obviously analogous to limitations of claim 117 (although a method or a computer-readable medium teaching a similar method is presented). Therefore, similar rationales and references set forth are applied for a rejection under 35 U.S.C. § 103(a).

16. Re. to Claims 134, 148, 164, 178: These claims' limitations are obviously analogous to limitations of claim 118 (although a method or a computer-readable medium

teaching a similar method is presented). Therefore, similar rationales and references set forth are applied for a rejection under 35 U.S.C. § 103(a).

17. Re. to Claims 135, 149, 165, 179: These claims' limitations are obviously analogous to limitations of claim 119 (although a method or a computer-readable medium teaching a similar method is presented). Therefore, similar rationales and references set forth are applied for a rejection under 35 U.S.C. § 103(a).

18. Re. to Claims 136, 150, 166, 180: These claims' limitations are obviously analogous to limitations of claim 120 (although a method or a computer-readable medium teaching a similar method is presented). Therefore, similar rationales and references set forth are applied for a rejection under 35 U.S.C. § 103(a).

19. Re. to Claims 137, 151, 167, 181: These claims' limitations are obviously analogous to limitations of claim 121 (although a method or a computer-readable medium teaching a similar method is presented). Therefore, similar rationales and references set forth are applied for a rejection under 35 U.S.C. § 103(a).

20. Re. to Claims 153, 123: These claims' limitations are obviously analogous to limitations of claim 107 (although a method or a computer-readable medium teaching a similar method is presented). Therefore, similar rationales and references set forth are applied for a rejection under 35 U.S.C. § 103(a).



21. Re. to Claims 154, 124: These claims' limitations are obviously analogous to limitations of claim 108 (although a method or a computer-readable medium teaching a similar method is presented). Therefore, similar rationales and references set forth are applied for a rejection under 35 U.S.C. § 103(a).

**Conclusion**

22. Claims 106-181 are not patentable.

23. These references are considered pertinent to applicants' disclosure.

- **Krishnan**, (US Pat. 6073124 - 6/06/2000), Method and system for securely incorporating electronic information into an online purchasing application

- **Stefik**, (US Pat. 5,715,403), discloses about a system for controlling the distribution and use of digital works having attached usage rights where the usage rights are defined by a usage rights grammar.

24. Any inquiry concerning this communication or earlier communications from the examiner should be directed to CUONG H. NGUYEN whose number is 703-305-4553. The examiner can normally be reached on 7am-3:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's acting supervisor, JEFFREY A. SMITH can be reached on 703-308-3588. The fax phone number for the organization where this application or proceeding is assigned is 703-305-7687 or 703-746-5572.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-308-1113.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Please provide support, with page and line numbers, for any amended or new claim in an effort to help advance prosecution; otherwise any new claim language that is introduced in an amended or new claim may be considered as new matter, especially if the Application is a Jumbo Application.

*Cuong H. Nguyen*

CUONG H. NGUYEN  
Primary Examiner  
Art Unit 3625